Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

Guidelines

on

Facsimile Transmission Security

June 1989

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

Fax: 416 965-2983
1-800-387-0073
Tel: 416 326-3333

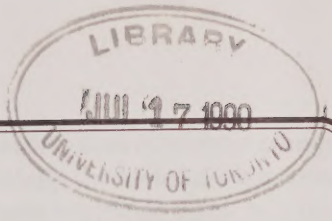

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

The facsimile (commonly referred to as "fax") is a widely used method of communicating information from one location to another. Essentially, the fax machine has the ability to send and receive copies of documents over ordinary telephone lines. In a typical fax transaction, the document to be faxed is placed in the document feeder of the fax unit; then the telephone number of the fax unit to which the document is to be sent is dialed. In a short time, a replica of the original document is printed out at the destination fax unit.

Situations have already occurred where documents have been inadvertently transmitted to the wrong destination. This can happen if the sender dials the wrong destination fax number, or if the intended recipient is not available to accept the faxed document and another person takes custody of it. Such situations not only raise the issue of compromised confidentiality, but also have implications for the *Freedom of Information and Protection of Privacy Act, 1987* (the *Act*). One of the purposes of the *Act* is to protect the privacy of individuals with respect to personal information about themselves held by government institutions. In the absence of specific directives, it is possible that government institutions may be using the fax to transmit sensitive, personal information. We are, in fact, aware of this very occurrence.

Recognizing these risks, the Office of the Information and Privacy Commissioner/ Ontario (IPC) has prepared a set of proposed guidelines for government institutions to consider when using the fax.

1.2 Objectives of this document

The purpose of this document is to set out guidelines for government institutions to consider when developing systems and procedures to maintain the confidentiality of information being transmitted by fax.

1.3 Approach

All organizations should have control over various activities that are performed within their organization. How they exercise this control varies from one organization to another. The objective is to ensure that desired events do take place (i.e. only authorized persons obtain access to sensitive information), and undesirable events do not take place (i.e. breaches of security). Clearly defined objectives enable an organization to achieve the desired level of control over its activities.

Specific control objectives necessary to maintain the confidentiality of information being transmitted have been explored. Attributes considered necessary to achieve these objectives are then identified.

1.4 Future Developments

While the security features associated with fax machines are relatively limited at the present time, the industry is in a state of flux, and significant developments in this area may be anticipated over the next year. The present guidelines will be updated in one year's time (or possibly earlier, if the need arises), to reflect any changes associated with new security features.

A recent development, that will undoubtedly increase in the absence of legislation, is what is popularly known as "junk fax". Organizations are using the fax to transmit unsolicited advertisements and press releases. This activity not only results in unwanted documents being received, but ties up the receiver's fax machine and uses up the receiver's stationary. In mid-May 1989 the State of Connecticut barred unsolicited advertising messages from being sent to fax machines in the state. Several other U.S. states are also in the process of considering similar legislation.

2. BACKGROUND DISCUSSION

2.1 Types of Information

All information held by government institutions does not require the same degree of security when communicated from one source to another. Thus, the first stage in the development of these guidelines was to categorize the various types of information held by government institutions.

The Government of Canada, in Part I section 3.1 of its Interim Security Standards: Operating Directives and Guidelines, categorizes information into:

- classified in the national interest; and
- protected but not in the national interest.

Unlike the federal government, the concept of "classified" or highly protected information does not exist within the Ontario government. Thus, for the purposes of these guidelines, the IPC used the requirements of the *Act* as the basis for categorizing information held by government institutions.

Under the *Freedom of Information and Protection of Privacy Act,1987*, records in the custody or control of a government institution in Ontario may be categorized as:

- Personal Information (Section 2 of the *Act*);
- Exempt Records (if they fall under Sections 12 through 22 of the *Act*);
- General Records (information other than Personal Information and Exempt Records as defined above).

Part III of the *Act*, which deals with the protection of individual privacy, requires that personal information held by institutions be protected from unauthorized use or disclosure, and regulates the collection, use, disclosure and disposal of personal information.

The *Act* also provides a right of access to a record or part of a record in the custody or control of a government institution, unless it falls within one of the exemptions contained in sections 12 through 22. Thus, exempt information should also be protected from unauthorized use or disclosure.

2.2 Existing Technology

At present, fax machines transmit and receive copies of documents over ordinary telephone lines. Therefore, like a telephone conversation, fax transmissions can be tapped and intercepted by unauthorized third parties. One method of avoiding this problem is for information to be encrypted or encoded so that it is rendered meaningless and cannot be read directly. The Government of Canada in Part III, Section B, Subsection 2.11.1, Interim Security Standards: Operating Directives and Guidelines, requires that classified information and other sensitive information designated as PROTECTED shall not be communicated in record communication systems, such as facsimile, unless the information has been cryptographically protected.

One of the manufacturers contacted by the IPC markets a fax with an encryption feature. This fax unit, however, can only transmit encrypted information between identical fax units. This consideration would thus appear to be far from practical at the present time for ordinary users.

Encrypted information may also be transmitted between computers and decrypted or decoded at the receiving computer. A fax attached to the destination computer could be used to print the transmitted information. A practical problem in using this procedure is that all the information required to be faxed may not be held on computers. For example, text such as minutes of meetings and other hand-written notes, may not be

stored on a computer. For such information to be faxed securely, it must first be transferred to a computer. Such a procedure is neither practical nor cost effective for ordinary users.

Therefore, under existing commercially available fax technology, encryption does not appear to be a satisfactory solution in most situations, but its use should be considered when sensitive information is involved.

2.3 Existing Capabilities of Fax Machines

Existing commercially-available fax technology and the scarcity of fax machines with a variety of security features have created limitations in achieving secure facsimile transmission.

Fax units are generally capable of printing a history of fax activity based on either a time span or volume of activity. For example, the fax unit can be set to automatically print a history of its activity after every 40 transactions.

This Fax Activity History Report is helpful in monitoring the use of the fax and to account for its activity. On most fax machines, however, once this report has been printed, it cannot be reprinted. As a result, it is possible for an unauthorized user to print these activity reports and destroy them, leaving no trace of unauthorized activity. A person could thus remove an incoming faxed document not intended for him, and eliminate any trace of the transaction by printing and destroying the activity report. Features do exist, however, on some fax machines which provide certain controls to overcome these problems.

i) Keylocks

The fax machine can be locked with a key. Unless it is unlocked, information cannot be transmitted nor can incoming information be printed. Thus, by installing a keylock, virtually all categories of information are subject to the same degree of security. This security procedure may not be practical where the fax has been acquired for general office use. There is also a risk that incoming information waiting to be printed can be lost in the case of a power loss to the fax. Manufacturers can provide an optional battery backup if required. In order to preserve information, certain models also store information on a data disk.

ii) Confidential Mailboxes

Certain fax units enable a document to be transmitted so that it can be received only by a specific person. This feature is commonly referred to as a "private or confidential mailbox". It is a memory location within the fax unit that stores incoming documents.

Practically, the number of confidential mailboxes in a fax unit is limited. The sender's fax unit must also be able to transmit to a fax unit with the same mailbox feature.

Documents can be transmitted to the intended receiver's confidential mailbox and printed out after a correct password is entered. This password is user-selected and can be changed by either supplying the old password or by using a master password held by the manufacturer. On most fax machines passwords are protected from loss due to temporary power lapses. However, the master password held by the manufacturer is usually the same for all of its products. Thus, it is possible for this master password to be widely known, thereby compromising security. In order to ensure confidentiality, the receiver would have to print the document immediately after it is received by the fax unit.

iii) Activity Confirmation Reports

Almost all fax machines print a confirmation of activity each time they are used. These reports confirm whether the transmission has been successful, and print the destination fax number and the number of pages transmitted. Thus, the sender can use it as some form of assurance that the documents have been transmitted correctly. The receiver can use the report to ensure that all transmitted pages have been received.

2.4 User Environment

The physical environment in which a fax is used may have a considerable impact on the security implications of fax transmissions. Offices sometimes situate their fax in a relatively public place where it can be used by virtually anyone, thus enabling unauthorized personnel to read incoming information. Such an environment makes it more difficult to maintain the confidentiality of personal information.

Another problem is that senders are usually completely unaware of the receiver's operating environment. The sender could fax confidential information on the presumption that the receiver's office procedures are secure, when in fact, they are not. Thus, non-standardized office procedures relating to fax use can result in the loss of confidentiality.

3. GUIDELINES

3.1 Personal Information and Exempt Records

Given the limitations of existing commercially-available fax technology, it is doubtful that the level of privacy protection required by the *Act* will be achieved. It is therefore recommended that personal information and exempt records, as defined in the *Act*, should **not** be transmitted by fax.

In emergency situations, where the recipient insists upon using fax as the mode of communication, the sender should send the information only to a confidential mailbox. This requirement is essential when transmitting highly sensitive, personal information. If a confidential mailbox is not available, personal information and exempt records should never be faxed.

However, if personal identifiers are removed from the document to be transmitted, then the document would no longer be considered "personal information", as defined by the *Act* . The removal of personal identifiers takes the information outside of the scope of "any information about an **identifiable** individual" and would thus enable the document to be faxed. Alternatively, the severance of personal information would also permit the faxing of documents of this nature.

3.2 General Records

i) **The fax machine should only be used by authorized persons.**

Persons authorized to use the fax would normally consist of office support staff. In a small to medium sized office, individual staff members may personally transmit documents. In a larger office, with a high volume of fax transmissions, consideration should be given to centralizing fax operations. By restricting use of the fax to authorized persons, the potential for unauthorized disclosure is reduced, should another office inadvertently fax confidential information.

- One person (and a backup) should be identified as responsible for all fax operations. Therefore, in case of problems, technical or otherwise, staff know who to contact.

- The fax machine should be located such that:

    - it is not in a public area;

    - its use can be monitored by the responsible person;

    - only authorized staff have access to information transmitted on the fax.

- Certain institutions may have to use the fax to communicate information requiring extra security protection. In these cases, the fax should be equipped with a keylock dedicated to this purpose.

- Fax machines should not be shared by institutions. Sharing results in the need to allocate or share confidential mailboxes, making it more difficult to maintain secure procedures.

ii) **Procedures should be implemented to ensure that information is sent to the intended fax number.**

Unlike erroneously addressed mail which may be returned unopened, a document faxed to the wrong number can be read by a number of people. In order to avoid this situation, institutions should take appropriate precautions to ensure that documents are directed to the correct fax number.

- A master list of authorized fax numbers should be maintained to serve as a reference list.

- The destination fax number should be reconfirmed before transmission. Unlike most ordinary telephones, the number being dialed from a fax unit is displayed on a screen similar to that on an electronic calculator. In existing fax machines, the destination fax number can be confirmed by physically checking the number displayed on the screen before transmitting the document.

- All fax machines used by government institutions should be able to print Fax Activity Confirmation Reports and Fax Activity History Reports.

- The sender should check the Fax Activity Confirmation Report for the accuracy of the destination fax number. This report should be retained with the original of the faxed document. Retaining the Fax Activity Confirmation Report provides a record that the document was faxed to the intended fax number.

- In case the document has been transmitted to the wrong fax number, the sender should immediately contact this organization, inform them of the error, and ensure that the faxed document is destroyed.

iii) Information should be transmitted completely and securely.

- The sender should confirm the success of the transmission by checking the Fax Activity Confirmation Report.

- All fax machines used by government institutions should be equipped with confidential mailboxes. Where confidentiality is required, information should be transmitted to a confidential mailbox. Government institutions should ascertain whether certain general records require extra protection because of their sensitivity.

iv) Information should reach the intended recipient.

Although information may be sent to the correct fax number, it could, nonetheless, reach the wrong recipient.

- The first page of all faxed documents should be a Fax Cover Sheet. It should identify the sender and the intended receiver. This page should eliminate any doubt regarding the intended receiver.

- The fax machine should be located so that only authorized persons can retrieve a document. (Refer to 3.2(1).)

- The receiver should initial the Fax Activity Confirmation Report. These reports should be in the custody of the person responsible for fax operations. (Refer to 3.2(1).)

- The person responsible for fax operations should review the Fax Activity Confirmation Reports (confirming receipt of a faxed document) to ensure that documents have been collected by the appropriate persons.

- In cases where a document has been transmitted to the wrong fax number, the recipient should inform the sender of the error, destroy the faxed document and note this action on the Fax Activity Confirmation Report. In cases where a document has been addressed to the wrong recipient, the actual recipient should re-direct the faxed document and make a corresponding notation on the Fax Activity Confirmation Report.

v) **Information should be received completely.**

- The receiver should check the number of pages actually received against the transmitted Fax Cover Sheet or against the Fax Activity Confirmation Report (in cases where no Fax Cover Sheet has been transmitted). If pages are missing, the sender should be contacted and asked to re-transmit the document.

- Consideration should be given to providing the fax with a battery backup in case of a power disruption. Institutions should consult their fax vendor.

- The fax machine should record on each page received:

  - the date and time received,
  - the fax number of the originator,
  - the name and identification of the originator, and
  - the page number of the document.

Sidney B. Linden
Commissioner

Ann Cavoukian, Ph.D.
Director of Compliance

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

GUIDELINES ON FACSIMILE TRANSMISSION SECURITY

EXECUTIVE SUMMARY

The facsimile (commonly referred to as "fax") is a widely used method of communicating information from one location to another. Recent incidents have occurred where documents were inadvertently transmitted to the wrong destination. Such situations not only raise the issue of compromised confidentiality, but also have implications for the *Freedom of Information and Protection of Privacy Act, 1987* (the "*Act*"). One of the purposes of the *Act* is to protect the privacy of individuals with respect to personal information about themselves held by government institutions. The Commissioner's office thought it was important at this time to develop proposed guidelines relating to fax security transmission, in order to preserve the confidentiality of information transmitted by fax.

A number of security features are available on fax machines such as key locks, confidential mail boxes, and encryption features, however most fax machines currently in use do not include these features.

The physical location of a fax machine has a significant impact on the security implications of fax transmissions. Offices often locate their fax in a relatively public place where it can be used by virtually anyone. This enables uncontrolled access to incoming fax information and creates potential problems in maintaining confidentiality of personal information. Also, the sender is usually unaware of the receiver's operating environment, thereby adding an additional level of concern.

... Guidelines on next page ...

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

Fax: 416 965-2983
1-800-387-0073
Tel: 416 326-3333